

[Date of request for examination]	17.02.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-183682

(P 2 0 0 2 - 1 8 3 6 8 2 A)

(43) 公開日 平成14年6月28日(2002.6.28)

(51) Int. Cl. 7	識別記号	F I	テーマコード (参考)
G06K 17/00		G06K 17/00	T 2C005
B42D 15/10	501	B42D 15/10	501 E 5B035
			501 P 5B058
G06K 19/10		G06K 19/00	R

審査請求 未請求 請求項の数 3 O L (全 6 頁)

(21) 出願番号 特願2000-385344 (P 2000-385344)

(22) 出願日 平成12年12月19日 (2000.12.19)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大西 基彦

東京都府中市東芝町1番地 株式会社東芝  
府中事業所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外 6 名)

F ターム (参考) 2C005 HA02 HB09 JA02 JB31 LA38

LB04 LB34

5B035 AA15 BB02

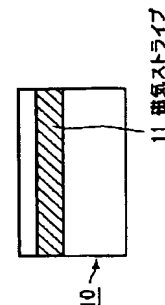
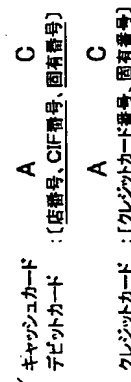
5B058 CA31 KA11 KA32

(54) 【発明の名称】 カード真偽判定装置

(57) 【要約】 (修正有)

【課題】 磁気カードのセキュリティ向上

【解決手段】 ホストは日時分秒等の動的パラメータに基づき真偽判定用の固有番号を作成し、磁気カード10とホストの双方に記録する。カード使用時、リーダは双方を照合して真偽判定した上、さらに先と同様の方法で新たに固有番号を作成し双方を更新する。動的パラメータ利用により、悪意の盗用者は固有番号作成法の類推が極めて困難になる。またカード使用ごとに固有番号が更新されるので、仮に作成法が類推できても現実的に盗用は困難である。



## 【特許請求の範囲】

【請求項1】 磁気カードに登録された情報と、照合用データベースの登録内容とに基づいて、前記磁気カードの真偽を判定するカード真偽判定装置であって、常に変動する動的パラメータに基づいて、前記磁気カード毎に固有番号情報を発行する手段と、前記発行された固有番号情報を前記磁気カード及び前記照合用データベースに登録する手段と、前記登録された固有番号情報に基づいて、前記磁気カードの真偽判定を行なう手段と、を備えたことを特徴とするカード真偽判定装置。

【請求項2】 請求項1に記載のカード真偽判定装置において、前記動的パラメータは、日時分秒を含む時間情報であることを特徴とするカード真偽判定装置。

【請求項3】 請求項1又は請求項2に記載のカード真偽判定装置において、前記磁気カードの使用される毎に、新たな固有番号情報を前記磁気カード及び前記照合用データベースに更新登録することを特徴とするカード真偽判定装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、クレジットカード、キャッシュカード及びデビットカード等の磁気カードを対象として（ICカードは対象外）、偽造カードの使用を防止でき、セキュリティ性を向上し得るカード真偽判定装置に関する。

## 【0002】

【従来の技術】通常、クレジットカード、キャッシュカード及びデビットカード等の磁気カードでは、操作入力される暗証番号及び磁気ストライプから読み出される情報（店番号・CIF番号等）をそれぞれデータベース内の情報と照合し、カードの真偽を判定するカード真偽判定装置が広く知られている。

【0003】しかし、このカード真偽判定装置は、磁気ストライプ内の情報と暗証番号との照合のみで真偽を判定するため、磁気ストライプ内の情報を読書き可能なカードリーダー装置の普及する現在、セキュリティが不十分と考えられている。

【0004】そこで、セキュリティ向上を図る観点から、例えば特開平10-255118号に開示されたエンボス読取装置のように、磁気カードのエンボス部をも含めて真偽判定を行なうカード真偽判定装置が考え出されている。

## 【0005】

【発明が解決しようとする課題】しかしながら以上のようなカード真偽判定装置では、エンボス部を含めて真偽判定を行なうものの、エンボス形成装置（エンボッサー）が市中で容易に安価に入手可能なため、エンボス部をも含めて偽造される可能性がある。

【0006】また、そもそも磁気カードを偽造するための、口座番号、店番号等の情報がカード表面のエンボス部に記載されるため、カード使用者がカードを紛失せず、に全く無過失であっても、知らないうちにカードを偽造され、不正使用される可能性を払拭できない。

【0007】従って、以上のように磁気カードには不正使用される可能性があるため、磁気カードのセキュリティ性を向上させる必要があると考えられる。本発明は上記実情を考慮してなされたもので、磁気カードのセキュリティ性を向上し得るカード真偽判定装置を提供することを目的とする。

## 【0008】

【課題を解決するための手段】本発明は、磁気カードに登録された情報と、照合用データベースの登録内容とに基づいて、前記磁気カードの真偽を判定するカード真偽判定装置であって、常に変動する動的パラメータに基づいて、前記磁気カード毎に固有番号情報を発行する手段と、前記発行された固有番号情報を前記磁気カード及び前記照合用データベースに登録する手段と、前記登録された固有番号情報に基づいて、前記磁気カードの真偽判定を行なう手段と、を備えたカード真偽判定装置である。

【0009】このように、常に変動する動的パラメータに基づいて、真偽判定用の固有番号情報を発行するので、磁気カード内の情報の算出ロジックを類推することが極めて困難になる。また、仮にロジックを類推できたとしても、算出に使用するパラメータに動的パラメータを使用することで、悪意の者が解析を図っても、現実的な盗用トライ回数からしても時間的に追いつくのが不可能であるため、磁気カードのセキュリティ性を向上できる。

【0010】また、前記動的パラメータは、日時分秒を含む時間情報であってもよい。これにより、上記作用を容易且つ確実に奏することができる。

【0011】さらに、前記磁気カードの使用される毎に、新たな固有番号情報を前記磁気カード及び前記照合用データベースに更新登録してもよい。これにより、悪意の者による固有番号情報の発見に要する想定時間よりも高頻度に固有番号情報が更新されると考えられるので、より一層、セキュリティ性を向上できる。

## 【0012】

【発明の実施の形態】以下、本発明の一実施形態について図面を参照しながら説明する。図1は本発明の一実施形態に係るカード真偽判定装置に適用される磁気カードの構成を示す模式図であり、図2は同カード真偽判定装置の一部である端末装置の構成を示す模式図であって、図3は同カード真偽判定装置の一部である照会ホスト装置の構成を示す模式図である。

【0013】すなわち、本実施形態に係る磁気カード10は、図1に示すように、従来の店番号及びCIF番号

を記載したエンボス部が省かれており、代わりに磁気ストライプ 11 内に店番号及び C I F 番号情報 A と、本発明特有の固有番号情報 C とが記録されている。

【0014】ここで、固有番号情報 C は、例えば、23 d i 9 4 j 5 f 1 2 Z C 9 の如きコード値であり、次式に示す如き、1 枚の磁気カード 10 毎に 1 つの固有番号を示している。

【0015】固有番号  $\equiv$  店番号 + C I F 番号 \* カード発行年 \* カード発行月 \* カード発行日 \* カード発行時 + カード発行分 \* カード発行秒 - 数値コード化された口座名義人の氏名 mod 大きな素数

固有番号は、理論的には複数のカードに対して一致することが、確率的に非常に希に起こり得るが、本発明においては問題とならない。特に、算出方法については、発行時分秒などを使用し、動的に固有番号が変化する仕組みであれば良く、上記数式には限定されない。

【0016】一方、本実施形態のカード真偽判定装置は、図 2 及び図 3 に示すように、複数の端末装置 20、20 a、20 b、…が通信手段を介して照会ホスト装置 30 に接続された構成となっている。なお、各端末装置 20、20 a、20 b、…は、カードの種類毎に同一構成なので、ここでは端末装置 20 を例に挙げて述べる。

【0017】ここで、端末装置 20 は、図 2 に示すように、磁気カード搬送機構部 21、磁気ストライプリーダ部 22、通信制御部 23、暗証番号入力部 24、磁気ストライプライト部 25 を備え、これら各部 21 ~ 25 を用いて、図 4 のフローチャートに示す処理を実行する機能をもっている。

【0018】この種の端末装置 20 は、具体的には例えば、クレジットカード照会端末 (C A T 端末) 機器、デビットカード端末機器、キャッシュカード端末 (銀行、郵便局 A T M) 機器などが使用可能である。なお、キャッシュカード端末機器の場合、暗証番号入力部は不要である。

【0019】磁気カード搬送機構部 21 は、磁気カード 10 の挿入・排出を行なう機能をもっている。

【0020】磁気ストライプリーダ部 22 は、磁気カード 10 の磁気ストライプ 11 から店番号・C I F 番号情報 A 及び固有番号情報 C を読み出す機能と、これら読み出した店番号・C I F 番号情報 A 及び固有番号情報 C を通信制御部 23 を介して照会ホスト装置 30 に送信する機能とをもっている。

【0021】通信制御部 23 は、照会ホスト装置 30 との間で情報の送受信を行なう機能をもっている。

【0022】暗証番号入力部 24 は、カード利用者の操作により、暗証番号情報 B が入力されると、この暗証番号情報 B を通信制御部 23 を介して照会ホスト装置 30 に送信する機能とをもっている。

【0023】磁気ストライプライト部 25 は、磁気ストライプ 11 中の固有番号情報 C を、照会ホスト装置 30

から受けた新たな固有番号情報 C に書き換える機能をもっている。

【0024】また一方、照会ホスト装置 30 は、顧客・カード照合データベース 31、取引用データベース 32、通信制御部 33、固有番号発生部 34、固有番号更新部 35、顧客・カード照合部 36 及び取引処理部 37 を備えている。

【0025】顧客・カード照合データベース 31 は、口座名義人毎に、店番号・C I F 番号情報 A、暗証番号 B 及び固有番号情報 C が登録されており、固有番号発生部 34、固有番号更新処理部 35、顧客・カード照合処理部 36 及び取引処理部 37 から読出／書込可能となっている。

【0026】取引用データベース 32 は、口座名義人毎に取引情報が登録されており、取引処理部 37 から読出／書込可能となっている。

【0027】通信制御部 33 は、各端末装置 20、20 a、20 b との間で情報の送受信を行なう機能をもっている。

【0028】固有番号発生部 34 は、日時分秒などの動的パラメータに基づいて、固有番号情報を発生するための演算部であり、取引処理部 37 による取引処理終了後、新たに発生させた固有番号情報 C を用いて、顧客・カード照合データベース内の固有番号情報 C を更新する機能をもっている。

【0029】固有番号更新処理部 35 は、固有番号発生部 34 により更新された顧客・カード照合データベース内の固有番号情報 C を通信制御部 33 を介して端末装置 20 に送信する機能をもっている。

【0030】顧客・カード照合部 36 は、端末装置 20 からそれぞれ送信された店番号・C I F 番号情報 A、暗証番号情報 B 及び固有番号情報 C に対し、顧客・カード照合データベース 31 の内容と照合する機能と、照合結果 (OK / NG) を端末装置 20 に送信する機能とをもっている。

【0031】取引処理部 37 は、端末装置 20 から受けた取引情報に基づいて、取引用データベース 32 を参照しながら取引処理を実行する機能をもっている。

【0032】次に、以上のように構成されたカード真偽判定装置の動作を図 4 のフローチャートを用いて説明する。利用者が磁気カード 10 を端末装置 20 に挿入したとする。端末装置 20 は、磁気カード搬送機構部 21 の動作により磁気カード 10 の挿入を検出すると (S T 1 ; y e s)、磁気ストライプリーダ部 22 により磁気カード 10 の磁気ストライプ 11 を読み取る (S T 2)。

【0033】続いて、端末装置 20 は、磁気カード 10 から読み取った店番号・C I F 番号情報 A 及び固有番号情報 C を通信制御部 23 を介して照会ホスト装置 30 に送信して照会する (S T 3)。

【0034】照会ホスト装置30は、店番号・CIF番号情報A及び固有番号情報Cを受取ると、顧客・カード照合処理部36が顧客・カード照合データベース31内の店番号・CIF番号情報A及び固有番号情報Cと、端末装置20から受けた店番号・CIF番号情報A及び固有番号情報Cとを照合し、照合結果（OK又はNG）を端末装置20に返信する。

【0035】端末装置20は、照合結果がNGであれば処理を終了するが、ここでは照合結果がOKである場合として、次に画面表示及び／又は音声案内などにより、暗証番号情報Bの入力をカード利用者に促す。

【0036】しかる後、端末装置20は、暗証番号情報Bが入力されると（ST4）、暗証番号情報Bを照会ホスト装置30に送信して照会する（ST5）。

【0037】照会ホスト装置30は、暗証番号情報Bを受けると、顧客・カード照合処理部36が顧客・カード照合データベース31の暗証番号情報Bと、端末装置20から受けた暗証番号情報Bとを照合し、照合結果（OK又はNG）を端末装置20に返信する。

【0038】端末装置20は、照合結果がNGであれば処理を終了するが、ここでは照合結果がOKである場合として、次に画面表示及び／又は音声案内などにより、取引情報の入力をカード利用者に促す。

【0039】端末装置20は、取引情報が入力されると、この取引情報及び店番号・CIF情報Aを照会ホスト装置30に送信して取引処理を実行する（ST6）。

【0040】照会ホスト装置30は、取引情報及び店番号・CIF情報Aを受けると、取引処理部37が取引用データベース32を参照して取引処理を実行し、取引結果を端末装置20に送信する。

【0041】端末装置20は、この取引結果を受けると、適宜、取引処理を終了し、その旨を照会ホスト装置30に通知する。

【0042】照会ホスト装置30は、取引処理の終了通知を受けると、固有番号発生部34が現在の日時分秒に基づいて、固有番号情報Cを別の番号に更新して顧客・カード照合データベース31を書換えると共に、固有番号更新処理部35が通信制御部33を介して更新後の固有番号情報Cを端末装置20に返信する。

【0043】端末装置20は、新たな固有番号情報Cを受けると（ST7）、磁気ストライプライト部25により磁気ストライプ11中の固有番号情報Cを更新後の内容に書換えて（ST8）、磁気カード搬送機構部21により磁気カード10を排出し、処理を終了する。

【0044】上述したように本実施形態によれば、カード利用者が磁気カード10の利用時、磁気カード10を端末装置に挿入すると、カード利用者が意識せずに、磁気カードストライプ11に書込まれた固有番号情報Cが照会ホスト装置30に送信され、顧客・カード照合データベース31内の登録内容と照合確認され、磁気カード

10の真偽判定が実行される。

【0045】ここで、固有番号情報Cが動的パラメータから得られたものであるので、悪意の者が、磁気カード10内の情報の算出ロジックを類推することが極めて困難になる。また、仮にロジックを類推できたとしても、算出に使用するパラメータに動的パラメータを使用することで、悪意の者が解析を図っても、現実的な盗用トライ回数からしても時間的に追いつくのが不可能である。よって、磁気カードのセキュリティ性を向上できる。

【0046】また、新規発行分カードのみならず、既発行済み使用中の磁気カード10においても、磁気カード10の使用時に照会ホスト装置30により、固有番号情報Cが自動的に別の値に更新されるので、悪意の者による固有番号情報の発見に要する想定時間よりも高頻度に固有番号情報が更新されると考えられ、より一層、セキュリティ性を向上できる。

【0047】なお、以上のようなカード真偽判定装置は、カード使用者に対し、何ら事務負担を加えることなく、既存のインフラベースで本方式へ移行できる利点をもつ。また、本物の磁気カード自体を入手しなければ盗用され難い利点をもつ。

【0048】さらに、上記カード真偽判定装置は、現在金融機関の一部でサービス提供されている、24時間対応のカード紛失時のフリーダイヤル受付、及び／又はATMによる暗証番号変更に供すれば、磁気カード利用者本人無過失による不正使用を格段に減少させることが期待できる。

【0049】なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【0050】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わせられた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0051】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0052】

【発明の効果】以上説明したように本発明によれば、磁気カードのセキュリティ性を向上できる。

【図面の簡単な説明】

【図 1】 本発明の一実施形態に係るカード真偽判定装置に適用される磁気カードの構成を示す模式図

【図 2】 同実施形態における端末装置の構成を示す模式図

【図 3】 同実施形態における照会ホスト装置の構成を示す模式図

【図 4】 同実施形態における動作を説明するためのフローチャート

【符号の説明】

10…磁気カード

11…磁気ストライプ

20, 20a, 20b…端末装置

21…磁気カード搬送機構部 21

22…磁気ストライプリーダ部 22

23, 33…通信制御部

24…暗証番号入力部

25…磁気ストライプライター部

30…照会ホスト装置

31…顧客・カード照合データベース

32…取引用データベース

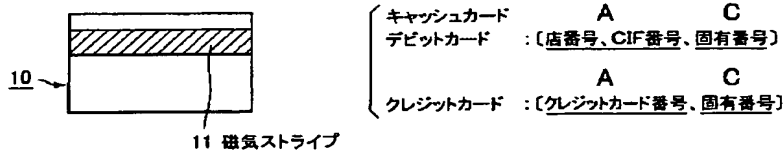
34…固有番号発生部

10 35…固有番号更新部

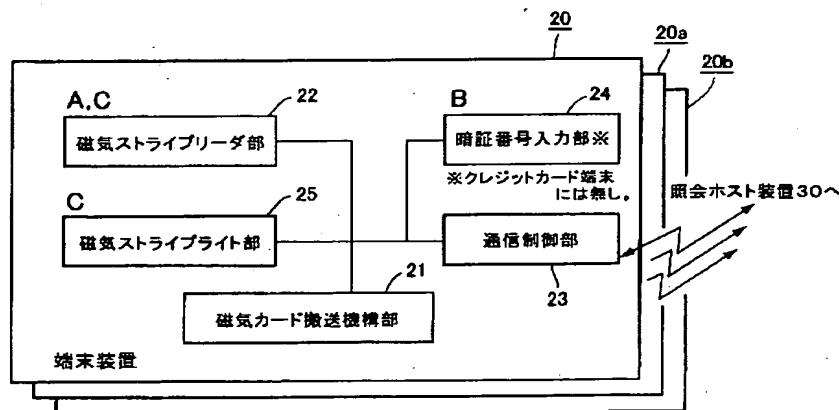
36…顧客・カード照合部

37…取引処理部

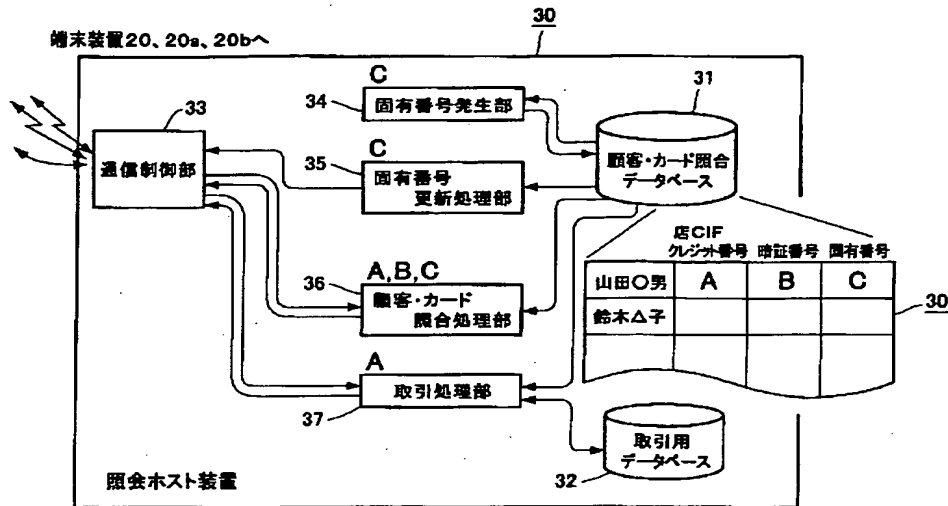
【図 1】



【図 2】



【図3】



【図4】

